

# EXHIBIT 14

## DECLARATION OF LAURENCE D. LIEB, OSFCE, MFCE

### Introduction

1. My name is Laurence D. Lieb. I am the President of Tyger Forensics Inc., which provides, among other things, computer forensics and electronic discovery services to litigation attorneys and their clients. I am a Passmark OSForensics Certified Examiner and a Magnet Forensics Certified Examiner. I am also a licensed private investigator in the State of Michigan.

2. To obtain my certification as an OSForensics Certified Examiner, I passed a certification testing process provided by Passmark. To remain certified, I am required, from time to time, to retrain and pass certification examinations for new software versions. A true and exact copy of my certification is attached as part of **Exhibit A** and incorporated by reference.

3. To obtain my certification as a Magnet Forensics Certified Examiner, I undertook online training led by Magnet Forensics. To remain certified, I am required, from time to time, to retrain and pass certification examinations for new software versions. A true and exact copy of my certification is attached as part of **Exhibit B** and incorporated by reference.

4. I counsel and assist clients in the preservation, extraction, and analysis of electronic data, using industry-standard practices, based on evidence personally analyzed, and form expert opinions regarding human interaction with electronic data from smartphones, computers, cloud-based sources, and a myriad of other electronic devices. I have been retained for this type of work around the country by numerous clients, as described in my curriculum vitae, which is attached as **Exhibit C**.

5. I have been retained by Ecolab, and its counsel, Fisher & Phillips LLP, to provide expert opinions regarding my forensic analysis of electronically stored information in the litigation titled ECOLAB Inc., and NALCO COMPANY, LLC d/b/a Nalco Water, an Ecolab Company

and/or Nalco Water, Plaintiffs, v. ANTHONY RIDLEY, and CHEMTREAT, INC, pending in the United States District Court, Eastern District of Tennessee, Chattanooga Division (the “Litigation”).

6. My hourly rate for this matter varies by task as follows: for pure forensic analysis & reporting, \$350 per hour; for written declarations, depositions, and other sworn testimony, \$450 per hour. My fees are unrelated to the outcome of the Litigation. My curriculum vitae, attached as **Exhibit C**, lists my testimonial experience for the last four years and all my publications for the last ten years.

7. This report is based on my personal knowledge, experience, and expertise in the area of forensic analysis of electronic devices. It is also based on my review of the documents and information contained within a log generated by ChemTreat’s endpoint security tool, CrowdStrike<sup>1</sup>, which was produced by Defendants as CHEMR-000002195.xml and a Western Digital MyBook Essential external USB hard drive, serial number WCAZA5437976, reported to belong to Anthony Ridley (“WD Drive”).

8. It is my understanding that the plaintiffs in this case are Ecolab, Inc. and Nalco Company, LLC (“Plaintiffs” or “Ecolab”), and the defendants are ChemTreat, Inc. (“ChemTreat”) and a former employee of Plaintiff named Anthony Ridley (“Ridley”). The claims pleaded by the Plaintiff, include (1) theft of trade secrets in violation of the Defend Trade Secrets Act, (2) violation of the Tennessee Uniform Trade Secrets Act, (3) breach of contract, (4) breach of fiduciary duty of loyalty, (5) tortious interference with contractual relationships, (6) procurement of breach of contract, (7) unfair competition, and (8) civil conspiracy. Plaintiffs claim that Ridley misappropriated trade secrets and other confidential information from Ecolab.

---

<sup>1</sup> <https://www.crowdstrike.com/products/endpoint-security/>

9. I reserve the right to render additional opinions, to supplement or amend the opinions in this report, and to provide additional grounds for those opinions based on my ongoing analysis of the materials provided to me or as may be required by events that occur during the course of this Litigation, including but not limited to responding to or analyzing positions taken by Ridley or his experts.

**CHEMR-000002195.XML Is Not Reasonably Accessible**

10. The file CHEMR-000002195.xml is expressly designed for ingestion and analysis by a CrowdStrike log analysis software program, not directly by a human being as I was required to do in this case. The fact that this log file was not designed for direct human consumption had a significant impact on my ability to search, analyze and report on the contents of CHEMR-000002195.xml as described below.

11. The creation of a searchable index by a computer forensic or electronic discovery tool enables one to search said index and perform complex searches such as Boolean searches, such as word “A” OR word “B,” word “A” AND word “B,” proximity searches, such as word “A” within five words of word “B,” and most critically the ability to search the index concurrently for thousands of search terms rather than having to search one word at a time.

12. I used three industry standard forensic tools, Magnet Forensics Axiom, Passmark’s OSForensics, and Vound Intella software, to generate a searchable index of CHEMR-000002195.xml and thus enable analysis. All three tools failed to create a searchable index of CHEMR-000002195.xml. CHEMR-000002195.xml is very large in size, specifically 314 megabytes and **contains 12,354,453 lines.**

13. Only one of the forensic tools, OSForensics, was able to open CHEMR-000002195.xml and allow me to run search terms, albeit one search term at a time.

14. For example, it took me two hours alone to search for the term “delete” as I had to left mouse click on the search arrow in OSForensics hundreds of times. I had to take a break after the two hours of left mouse clicking during the search for responsive hits containing the term “delete” as my hand was aching at the end of two hours. Ultimately I found no evidence of file deletion in the CrowdStrike log as claimed by Mr. Ridley in his deposition.

15. I spoke with three CrowdStrike representatives on February 7, 2023 to see if CrowdStrike would provide me with a free license of their log analysis software to ingest the CHEMR-000002195.xml XML log and thus enable me to perform forensic analysis using CrowdStrike software. Unlike Microsoft Excel XLSX files, XML files such as CHEMR-000002195.xml, are not designed for human consumption, but rather are explicitly designed to be opened and analyzed by specialized software programs. XML stands for “extensible markup language” and is a file format used, for example, to build web pages which can then be opened by an internet browser. CrowdStrike sells a specific log analysis tool to corporate clients which could be used to open and analyze the CHEMR-000002195.xml file, but the CrowdStrike log analysis software costs thousands of dollars including an annual subscription, and CrowdStrike unfortunately was not willing to provide me with a trial version.

16. I have included a screenshot of CHEMR-000002195.xml below to demonstrate why this XML file is not designed to be opened and analyzed directly by a human being.

### **Screenshot of CHEMR-000002195.xml as opened by OSForensics**

```
<result offset='74510'>
  <field k='_time'>
    <value> <text>2022-02-20T19:28:53.866+0000</text></value>
  </field>
  <field k='name'>
    <value> <text>KernelModeLoadImageV11</text></value>
  </field>
</result>
<result offset='74511'>
  <field k='_time'>
    <value> <text>2022-02-20T19:28:53.866+0000</text></value>
  </field>
  <field k='name'>
    <value> <text>NewExecutableWrittenV2</text></value>
  </field>
  <field k='TargetFileName'>
    <value> <text>\Device\HarddiskVolume3\Users\anthony.ridley\AppData\Roaming\Microsoft\Windows\Recent\Nalco.lnk</text></value>
  </field>
```

### **Identification of Additional USB Drives and an Apple iPad within the CrowdStrike log**

17. After the publication of my original expert report and my rebuttal to James Vaughn's report, I was able to identify even more USB drives and an Apple iPad having been connected to the wiped ChemTreat laptop within the CHEMR-000002195.xml file. I have included all eight devices in Table A below.

#### **Table A – Devices Attached to The Wiped ChemTreat Laptop**

- (1) a Lexar USB Flash Drive serial number 040GTDACGOJI9EN6,
- (2) a Lexar USB Flash Drive serial number 56261F6B34AF1760
- (3) a Western Digital My Book 1130 serial number 5743415A4135343337393736
- (4) a UDisk USB Drive (UDisk is a manufacturer of generic USB drives); the CrowdStrike log did not capture a serial number for this UDisk drive.
- (5) a generic USB Flash Disk drive, serial number 0416080000012762

- (6) a PNY Technologies model USB 2.0 FD serial number AA00000000017935
- (7) an AmazonBasics Hard Drive Enclosure serial number 180129000600
- (8) an Apple iPad serial number d7a686b5d025f71524c7f4840107bd7c2a59e6dd

18. The James Vaughn report never mentions the **Lexar USB Flash Drive**, serial number **040GTDACGOJI9EN6** notwithstanding the fact that CrowdStrike log contained evidence of this drive being connected to the wiped ChemTreat laptop on July 12, 2021 as seen in the below screenshot taken directly from the CrowdStrike log.

**Lexar USB Flash Drive serial number 040GTDACGOJI9EN6 Connected 7/12/2021**

```
<result offset='1493608'>
  <field k='_time'>
    <value><text>2021-07-12T12:52:03.723+0000</text></value>
  </field>
  <field k='name'>
    <value><text>DcUsbDeviceConnectedV2</text></value>
  </field>
  <field k='DeviceManufacturer'>
    <value><text>Lexar</text></value>
  </field>
  <field k='DeviceProduct'>
    <value><text>USB Flash Drive</text></value>
  </field>
  <field k='DeviceSerialNumber'>
    <value><text>040GTDACGOJI9EN6</text></value>
  </field>
</result>
```

19. The James Vaughn report never mentions the Lexar USB Flash Drive serial number 56261F6B34AF1760, notwithstanding the fact that the CrowdStrike log contains evidence of this Lexar drive having been connected to the wiped ChemTreat laptop on October 29, 2021 as seen in the screenshot below taken directly from the CrowdStrike log.

**Lexar USB Flash Drive serial number 56261F6B34AF1760 Connected 10/29/2021**

```
</result>
<result offset='863199'>
  <field k='_time'>
    <value><text>2021-10-29T14:33:55.066+0000</text></value>
  </field>
  <field k='name'>
    <value><text>DcUsbDeviceConnectedV2</text></value>
  </field>
  <field k='DeviceManufacturer'>
    <value><text>Lexar</text></value>
  </field>
  <field k='DeviceProduct'>
    <value><text>USB Flash Drive</text></value>
  </field>
  <field k='DeviceSerialNumber'>
    <value><text>56261F6B34AF1760</text></value>
  </field>
</result>
```

20. The James Vaughn report never mentions the PNY Technologies model USB 2.0 FD serial number AA00000000017935 notwithstanding the fact that the CrowdStrike log contained evidence of this drive being connected to the wiped ChemTreat laptop on October 1, 2021 as seen in the screenshot below taken directly from the CrowdStrike log.



**PNY Technologies USB 2.0 FD serial number AA00000000017935 Connected 10/1/2021**

```
<result offset='1041020'>
  <field k='_time'>
    <value><text>2021-10-01T13:15:25.132+0000</text></value>
  </field>
  <field k='name'>
    <value><text>DcUsbDeviceConnectedV2</text></value>
  </field>
  <field k='DeviceManufacturer'>
    <value><text>PNY Technologies</text></value>
  </field>
  <field k='DeviceProduct'>
    <value><text>USB 2.0 FD</text></value>
  </field>
  <field k='DeviceSerialNumber'>
    <value><text>AA00000000017935</text></value>
  </field>
</result>
```

21. The James Vaughn report never mentions the **UDisk** drive notwithstanding the fact that the CrowdStrike log contained evidence of the **UDisk** drive being connected to the wiped ChemTreat laptop on two different dates, **July 22, 2021** and **October 1, 2021**, as seen in the two CrowdStrike screenshots below.

### UDisk Connected to Wiped ChemTreat Laptop on 07/22/2021

```
<result offset='1435006'>
  <field k='_time'>
    <value><text>2021-07-22T08:47:11.429+0000</text></value>
  </field>
  <field k='name'>
    <value><text>DcUsbDeviceConnectedV2</text></value>
  </field>
  <field k='DeviceManufacturer'>
    <value><text>General </text></value>
  </field>
  <field k='DeviceProduct'>
    <value><text>UDisk </text></value>
  </field>
  <field k='DeviceSerialNumber'>
    <value><text>D%</text></value>
  </field>
</result>
```

### UDisk Connected to Wiped ChemTreat Laptop on 10/01/2021

```
<result offset='1041070'>
  <field k='_time'>
    <value><text>2021-10-01T13:14:14.513+0000</text></value>
  </field>
  <field k='name'>
    <value><text>DcUsbDeviceConnectedV2</text></value>
  </field>
  <field k='DeviceManufacturer'>
    <value><text>General </text></value>
  </field>
  <field k='DeviceProduct'>
    <value><text>UDisk </text></value>
  </field>
  <field k='DeviceSerialNumber'>
    <value><text>D%</text></value>
  </field>
</result>
```

22. As detailed in my original report, my forensic tool OSForensics was able to carve and recover deleted multiple files from the UDisk drive, which was originally provided to me by Mr. Ridley's counsel. I subsequently created a forensic image of this UDisk drive and provided a copy of the forensic image to James Vaughn. I was also able to recover multiple Nalco files from the UDisk drive itself as detailed below.

23. OSForensics was able to carve a deleted PDF file from the UDisk, which I have attached as Exhibit D. **Exhibit D**, titled “District Manager Sales Planning Guide” clearly bears the Nalco logo and also the text “CONFIDENTIAL - For Internal Use Only”.

24. OSForensics was able to carve a second deleted PDF file from the UDisk, which I have attached as Exhibit E. **Exhibit E**, titled “Sales Strategies and Techniques” clearly bears the Nalco logo and also the text “CONFIDENTIAL - For Internal Use Only”.

25. OSForensics was able to carve a third deleted PDF file from the UDisk, which I have attached as Exhibit F. **Exhibit F**, titled “Proposal for Reverse Osmosis System and Boiler/Cooling Program” clearly bears the Nalco logo.

26. OSForensics was able to carve a fifth deleted PDF file from the UDisk, which I have attached as Exhibit G. **Exhibit G**, titled “Pilgrim's-JBS Boiler Operator Training Final 4kwk” clearly bears the Nalco logo and contains the text “Confidential”. Exhibit G has the exact same file name of a file exfiltrated by Ridley from Ecolab on May 26, 2021 as recorded by the Ecolab Digital Guardian report.

27. Forensic analysis of the CrowdStrike log revealed the fact that the UDisk drive was connected to Ridley’s first wiped ChemTreat laptop on **July 22, 2021** and **October 10, 2021**.

28. Forensic analysis of Ridley’s second ChemTreat laptop revealed the fact that **this UDisk drive was never connected to the second ChemTreat laptop**.

29. Forensic analysis of the UDisk revealed the fact that Ridley deleted a file named “\_ESKTOP.INI” from a folder named “**Files from Ridley's personal computer**” on **February 9, 2022** at 3:34 PM CST as seen in the table below from OSForensics.

Filename	Location	Created	Modified	Timezone
ESKTOP.INI	USB001:\Files from Ridley's personal computer\Pictures\	2/9/22 3:34 PM	2/9/22 3:34 PM	-5:00
ESKTOP.INI	USB001:\Files from Ridley's personal computer\Music\	2/9/22 3:34 PM	2/9/22 3:34 PM	-5:00

30. Ridley claims in his deposition that he does not own a personal home computer.

31. **Therefore, Ridley must have used an undisclosed computer on February 9, 2022 to delete the files contained on the UDisk drive.**

32. Mr. Vaughn opines that the CrowdStrike log reliably recorded all human interaction with files stored on USB drives connected to ChemTreat laptops. Therefore, Mr. Vaughn wishes us to believe that Mr. Ridley connected the UDisk drive to his wiped ChemTreat laptop on two different dates but never interacted with files on the UDisk drive, notwithstanding the fact that the UDisk drive indisputably contains multiple files bearing the Nalco logo and the word “Confidential”. As I explain in detail below, the CrowdStrike log itself and Mr. Vaughn’s validation of the CrowdStrike tool using a test laptop entirely omits multiple types of human interaction, such as printing files to paper using a printer.

33. The James Vaughn report never mentions the AmazonBasics Hard Drive Enclosure serial number 180129000600 notwithstanding the fact that CrowdStrike logged this drive being connected to the wiped ChemTreat laptop on **July 9, 2021** as seen in the CrowdStrike screenshot below.

**AmazonBasics Hard Drive Enclos DeviceSerialNumber 180129000600 Connected 7/9/2021**

```
<result offset='1501294'>
  <field k='_time'>
    <value><text>2021-07-09T10:20:40.364+0000</text></value>
  </field>
  <field k='name'>
    <value><text>DcUsbDeviceConnectedV2</text></value>
  </field>
  <field k='DeviceManufacturer'>
    <value><text>AmazonBasics</text></value>
  </field>
  <field k='DeviceProduct'>
    <value><text>AmazonBasics Hard Drive Enclos</text></value>
  </field>
  <field k='DeviceSerialNumber'>
    <value><text>180129000600</text></value>
  </field>
</result>
```

34. The James Vaughn report never mentions the Apple iPad serial number d7a686b5d025f71524c7f4840107bd7c2a59e6dd notwithstanding the fact that the CrowdStrike log contains evidence of this iPad having been connected to the wiped ChemTreat laptop on **August 3, 2021** and **October 21, 2021** as seen in the CrowdStrike screenshot below.

**Apple Inc iPad serial number d7a686b5d025f71524c7f4840107bd7c2a59e6dd Connected 08/03/2021**

```
</result>
<result offset='1380191'>
  <field k='_time'>
    <value><text>2021-08-03T21:40:12.524+0000</text></value>
  </field>
  <field k='name'>
    <value><text>DcUsbDeviceConnectedV2</text></value>
  </field>
  <field k='DeviceManufacturer'>
    <value><text>Apple Inc.</text></value>
  </field>
  <field k='DeviceProduct'>
    <value><text>iPad</text></value>
  </field>
  <field k='DeviceSerialNumber'>
    <value><text>d7a686b5d025f71524c7f4840107bd7c2a59e6dd</text></value>
  </field>
</result>
```

**Apple Inc iPad serial number d7a686b5d025f71524c7f4840107bd7c2a59e6dd Connected 10/21/2021**

```
<result offset='911265'>
  <field k='_time'>
    <value><text>2021-10-21T19:58:40.998+0000</text></value>
  </field>
  <field k='name'>
    <value><text>DcUsbDeviceDisconnectedV2</text></value>
  </field>
  <field k='DeviceManufacturer'>
    <value><text>Apple Inc.</text></value>
  </field>
  <field k='DeviceProduct'>
    <value><text>iPad</text></value>
  </field>
  <field k='DeviceSerialNumber'>
    <value><text>d7a686b5d025f71524c7f4840107bd7c2a59e6dd</text></value>
  </field>
```

35. The Vaughn report never mentions a generic USB Flash Disk drive, serial number 0416080000012762, notwithstanding the fact that the CrowdStrike log contained evidence of this

drive being connected to the wiped ChemTreat laptop on **July 22, 2022** and **October 1, 2022** as seen in the screenshot below from the CrowdStrike log.

**Generic USB Flash Disk drive, serial number 0416080000012762 Connected 07/22/2022**

```
<result offset='1434977'>
  <field k='_time'>
    <value><text>2021-07-22T08:48:13.049+0000</text></value>
  </field>
  <field k='name'>
    <value><text>DcUsbDeviceConnectedV2</text></value>
  </field>
  <field k='DeviceManufacturer'>
    <value><text>General</text></value>
  </field>
  <field k='DeviceProduct'>
    <value><text>USB Flash Disk</text></value>
  </field>
  <field k='DeviceSerialNumber'>
    <value><text>0416080000012762</text></value>
  </field>
</result>
```

**Generic USB Flash Disk drive, serial number 0416080000012762 Connected 10/01/2022**

```
<result offset='1040979'>
  <field k='_time'>
    <value><text>2021-10-01T13:16:02.836+0000</text></value>
  </field>
  <field k='name'>
    <value><text>DcUsbDeviceConnectedV2</text></value>
  </field>
  <field k='DeviceManufacturer'>
    <value><text>General</text></value>
  </field>
  <field k='DeviceProduct'>
    <value><text>USB Flash Disk</text></value>
  </field>
  <field k='DeviceSerialNumber'>
    <value><text>0416080000012762</text></value>
  </field>
</result>
```



36. I was provided with this exact USB drive by Ridley's counsel, and subsequently created a forensic image of this drive and provided a copy of the forensic image to James Vaughn.

37. OSForensics was able to carve and recover a file named "Ridley Contacts.CSV" from generic USB Flash Disk drive, serial number 0416080000012762. Forensic analysis of the OSForensics index showed that Ridley deleted this "Ridley Contacts.CSV" from this USB drive on February 9, 2022.

38. Forensic analysis of the CrowdStrike log identified evidence of Ridley opening a file named "Ridley Contacts" on October 1, 2021 from a generically named "USB DISK (D)" as seen in the CrowdStrike log screenshot below. Nowhere in the Vaughn report is any mention of this file interaction nor usage of this USB drive.

```
</result>
<result offset='1040878'>
  <field k='_time'>
    <value><text>2021-10-01T13:19:03.354+0000</text></value>
  </field>
  <field k='name'>
    <value><text>NewExecutableWrittenV1</text></value>
  </field>
  <field k='TargetFileName'>
    <value><text>\Device\HarddiskVolume3\Users\anthony.ridley\AppData\Roaming\Microsoft\Windows\Recent\Ridley Contacts.lnk</text></value>
  </field>
</result>
<result offset='1040879'>
  <field k='_time'>
    <value><text>2021-10-01T13:19:03.354+0000</text></value>
  </field>
  <field k='name'>
    <value><text>NewExecutableWrittenV1</text></value>
  </field>
  <field k='TargetFileName'>
    <value><text>\Device\HarddiskVolume3\Users\anthony.ridley\AppData\Roaming\Microsoft\Windows\Recent\USB DISK (D).lnk</text></value>
  </field>
</result>
```

39. Forensic analysis of the CrowdStrike log identified a person I assume to be Anthony Ridley accessing a folder named "Nalco" by clicking on a "link" ".lnk" shortcut file seven different times on February 9<sup>th</sup>, 2022 and once on February 20, 2022 as seen in the below screenshots taken directly from the CrowdStrike log.

40. It is important to note that the “Nalco” folder Ridley accessed eight times by clicking on the “Nalco.lnk” shortcut file did not exist on a USB drive attached to the wiped ChemTreat laptop. Therefore, Ridley must have had a folder called “Nalco” on his (wiped) ChemTreat laptop, in a personal OneDrive account, or his ChemTreat OneDrive account.

**Ridley Access a “Nalco” folder on 2022-02-09T14:11:07.531+0000**

```
<result offset='145347'>
  <field k='_time'>
    <value><text>2022-02-09T14:11:07.531+0000</text></value>
  </field>
  <field k='name'>
    <value><text>NewExecutableWrittenV2</text></value>
  </field>
  <field k='TargetFileName'>
    <value><text>\Device\HarddiskVolume3\Users\anthony.ridley\AppData\Roaming\Microsoft\Windows\Recent\Nalco.lnk</text></value>
  </field>
</result>
```

**Ridley Access a “Nalco” folder on 2022-02-09T14:12:11.648+0000**

```
<result offset='145289'>
  <field k='_time'>
    <value><text>2022-02-09T14:12:11.648+0000</text></value>
  </field>
  <field k='name'>
    <value><text>NewExecutableWrittenV2</text></value>
  </field>
  <field k='TargetFileName'>
    <value><text>\Device\HarddiskVolume3\Users\anthony.ridley\AppData\Roaming\Microsoft\Windows\Recent\Nalco.lnk</text></value>
  </field>
</result>
```

**Ridley Access a “Nalco” folder on 2022-02-09T14:13:50.621+0000**

```
<result offset='145218'>
  <field k='_time'>
    <value><text>2022-02-09T14:13:50.621+0000</text></value>
  </field>
  <field k='name'>
    <value><text>NewExecutableWrittenV2</text></value>
  </field>
  <field k='TargetFileName'>
    <value><text>\Device\HarddiskVolume3\Users\anthony.ridley\AppData\Roaming\Microsoft\Windows\Recent\Nalco.lnk</text></value>
  </field>
</result>
<result offset='145219'>
```



### **Ridley Access a “Nalco” folder on 2022-02-09T14:14:11.125+0000**

```
<result offset='145205'>
  <field k='_time'>
    <value><text>2022-02-09T14:14:11.125+0000</text></value>
  </field>
  <field k='name'>
    <value><text>NewExecutableWrittenV2</text></value>
  </field>
  <field k='TargetFileName'>
    <value><text>\Device\HarddiskVolume3\Users\anthony.ridley\AppData\Roaming\Microsoft\Windows\Recent\Nalco.Ink</text></value>
  </field>
</result>
```

### **Ridley Access a “Nalco” folder on 2022-02-09T14:15:07.909+0000**

```
<result offset='145164'>
  <field k='_time'>
    <value><text>2022-02-09T14:15:07.909+0000</text></value>
  </field>
  <field k='name'>
    <value><text>NewExecutableWrittenV2</text></value>
  </field>
  <field k='TargetFileName'>
    <value><text>\Device\HarddiskVolume3\Users\anthony.ridley\AppData\Roaming\Microsoft\Windows\Recent\Nalco.Ink</text></value>
  </field>
</result>
```

### **Ridley Access a “Nalco” folder on 2022-02-09T14:16:08.970+0000**

```
<result offset='145128'>
  <field k='_time'>
    <value><text>2022-02-09T14:16:08.970+0000</text></value>
  </field>
  <field k='name'>
    <value><text>NewExecutableWrittenV2</text></value>
  </field>
  <field k='TargetFileName'>
    <value><text>\Device\HarddiskVolume3\Users\anthony.ridley\AppData\Roaming\Microsoft\Windows\Recent\Nalco.Ink</text></value>
  </field>
</result>
```

### **Ridley Access a “Nalco” folder on 2022-02-09T19:33:12.903+0000**

```
<result offset='142301'>
  <field k='_time'>
    <value><text>2022-02-09T19:33:12.903+0000</text></value>
  </field>
  <field k='name'>
    <value><text>NewExecutableWrittenV2</text></value>
  </field>
  <field k='TargetFileName'>
    <value><text>\Device\HarddiskVolume3\Users\anthony.ridley\AppData\Roaming\Microsoft\Windows\Recent\Nalco.Ink</text></value>
  </field>
</result>
```

**Ridley Access a “Nalco” folder on 2022-02-20T19:28:53.866+0000**

```
<result offset='74511'>
  <field k='_time'>
    <value><text>2022-02-20T19:28:53.866+0000</text></value>
  </field>
  <field k='name'>
    <value><text>NewExecutableWrittenV2</text></value>
  </field>
  <field k='TargetFileName'>
    <value><text>\Device\HarddiskVolume3\Users\anthony.ridley\AppData\Roaming\Microsoft\Windows\Recent\Nalco.Ink</text></value>
  </field>
</result>
```

41. Based on my analysis and James Vaughn’s comments regarding the CrowdStrike log, it is highly likely that the “Nalco” folder referenced above was on Ridley’s ChemTreat laptop.

42. Also, the CrowdStrike log shows no evidence of the “Nalco” folder being created and no evidence of the files that Ridley interacted with when accessing the “Nalco” folder on February 9, 2022 or any other date.

43. Further, Mr. Vaughn’s report never mentions any of this activity on February 9, 2022 in volving the “Nalco” folder (or any other activity on that same date).

**Analysis of “Personnel” or “Personal” Files Identified by the Digital Guardian Report**

44. Ridley states in his deposition, Page 167, lines 8-22, “And I wanted to make sure that the Nalco Water files were properly preserved and would be properly segregated to the correct individuals and that they would not be mixed with the Ecolab files because it was two separate businesses. It was – there were little to -- there were actually no overlap between the two. And included with those Nalco files, because I was a district manager, there were extensive amount of personnel files that did not need to make it into the view of someone who potentially took over my next business or my next book of business with Ecolab because I had seen that happen. I had experienced it personally.”

45. Accordingly, I analyzed the Digital Guardian report to identify the “personnel” files Ridley was referencing. Using the exact search term “personnel” returned zero positive hits in the Digital Guardian report.

**The Ridley Deposition Testimony Does Not Match the CrowdStrike Log**

46. I analyzed the Ridley deposition and compared Ridley’s testimony to evidence contained in the CrowdStrike log.

47. On Page 100, Ridley states that “I did delete -- I grabbed a large block of files and deleted what I found during each session.”

48. Forensic analysis of the CrowdStrike log identified no evidence of deletion of files by Ridley.

49. James Vaughn’s expert report contains no reference to evidence of file deletion by Ridley, notwithstanding the fact that Vaughn asserts, incorrectly in my opinion, that the CrowdStrike log recorded all human interaction with files contained on USB drives.

50. On Page 105, Ridley states that “I believe I was actually putting some pictures from a deer camera on the computer.”

51. Forensic analysis of the CrowdStrike log identified no evidence of Ridley accessing a picture file with the term “deer” in the picture file name.

52. Forensic analysis identified only two picture files named “IMG\_1864.JPG” and “Headshot from 2015.JPG” being accessed from an external USB drive on July 21, 2022 as seen in the CrowdStrike screenshot below.

```

</result>
<result offset='1444275'>
  <field k='_time'>
    <value><text>2021-07-21T21:09:23.602+0000</text></value>
  </field>
  <field k='name'>
    <value><text>RansomwareOpenFileV4</text></value>
  </field>
  <field k='TargetFileName'>
    <value><text>\Device\HarddiskVolume5\My Pictures\Pictures\Headshot from 2015.JPG</text></value>
  </field>
</result>

</result>
<result offset='1444353'>
  <field k='_time'>
    <value><text>2021-07-21T21:02:54.062+0000</text></value>
  </field>
  <field k='name'>
    <value><text>RansomwareOpenFileV4</text></value>
  </field>
  <field k='TargetFileName'>
    <value><text>\Device\HarddiskVolume5\My Pictures\924BJHKG\IMG_1864.JPG</text></value>
  </field>
</result>

```

53. Please note that the above CrowdStrike screenshot contains the words, “RansomwareOpenFileV4,” which underlines the fact that CrowdStrike is an endpoint security and malware detection tool designed to protect customers from hackers and viruses, not a data loss prevention tool as Vaughn incorrectly asserts. Ransomware is a form of malware criminals use to maliciously encrypt victims’ computer systems.

54. On Page 106 of his deposition, Ridley states in response to a question, “All right. In September 2021, when you deleted other documents off the WD drive using your ChemTreat computer, why did you initially attach the WD drive to your ChemTreat computer?” that “Same reason as earlier. I was putting pictures on the computer.”

55. Forensic analysis of the CrowdStrike log revealed no evidence of Ridley accessing pictures from an external USB drive and copying pictures to the wiped ChemTreat’s internal hard drive in September of 2021.

56. The Vaughn report makes no mention of the picture access and copying activity Ridley testified to having performed in September of 2021 whatsoever.

57. On Page 110 of the Ridley deposition, Ridley states that in January of 2022, he “Started clicking and segregating things into folders and dragging things into folders.” on the Western Digital drive when the Western Digital drive was attached to the wiped ChemTreat laptop.

Q. Sure. In January 2022 when you deleted Nalco files, Nalco/Ecolab files from the WD drive, what specifically – what specifically occurred then?

A. I clicked on the files, and at that time I actually started -- since this was -- I now found files three times prior to that, I actually went in and started kind of sorting a few things and making sure nothing else was left -- nothing else was remaining on the WD.”

Q. How specifically did you do that?

A. Started clicking and segregating things into folders and dragging things into folders.

58. Forensic analysis of the CrowdStrike log revealed no evidence whatsoever of Ridley segregating or dragging files into folders.

59. The Vaughn report contains no reference whatsoever to Ridley segregating or dragging files into folders in January 2022 using the Western Digital drive attached to the wiped ChemTreat laptop.

60. In my opinion, either Ridley gave inaccurate testimony about segregating or dragging files on the Western Digital drive as it was connected to the wiped ChemTreat laptop in January 2022, or the CrowdStrike log did not record this significant file interaction and thus Vaughn’s assertion that the CrowdStrike log is a reliable source of all human interaction with files on USB drives connected to ChemTreat laptops is not correct. Both cannot be true.

61. On Page 112 of the Ridley deposition, Ridley testifies to having spent more than one hour “looking through the majority of files” on the Western Digital drive and then deleting Nalco/Ecolab files in January of 2022.

Q. Okay. And then after you delete -- so at that point, did you delete some of the folders or some of the Nalco/Ecolab files in January 2022?

A. Files were deleted in January of 2022.

Q. So you organized them first and then you deleted them.

A. No. Deletion happened first.

Q. Okay.

A. To my knowledge.

Q. And do you know how many files that you deleted during that session?

A. I do not.

Q. What did you do to make sure that there wasn't anything else on there that related to Nalco or Ecolab?

A. I looked through the majority of the -- I looked through the files on there and could not find anything else.

Q. You started to say "the majority." Did you look at all the files?

A. I did the best I could to look through all the files and did a search of the device to see if any were on there.

Q. Sitting here today, are you a hundred percent certain that there were no Nalco or Ecolab documents on that drive?

A. Yes.

Q. Why are you certain?

A. To my knowledge, in the looks that I've done -- and I've gone through

Q: More than an hour?

A. Probably, yes.

62. Forensic analysis of the CrowdStrike log evidence of Ridley opening only two files from the Western Digital drive in January of 2022, a file named “~\$LCO Master Proposal.dotm”<sup>2</sup> and a file named “~\$mote Service Plan-2020 v1.docx”.<sup>3</sup> Forensic analysis revealed no evidence whatsoever of Ridley deleting multiple Nalco/Ecolab files from the Western Digital drive in January of 2022.

63. The Vaughn report contains no reference whatsoever to Ridley having deleted multiple Nalco/Ecolab files from the Western Digital drive in January of 2022.

64. On page 333 of the Ridley deposition, Ridley testifies that he deleted a file from the Western Digital drive.

---

<sup>2</sup> CrowdStrike log offset 239958

<sup>3</sup> CrowdStrike log offset 239960

Q. All right. So then the next document is Device Hard Disk Volume 6\Nalco Water Files\service report notes\service report technical notes - version 3.docx. Do you remember opening that document?

A. Yes.

Q. When did you open that document?

A. When I found those on the WD and then reviewed them and deleted them.

65. Forensic analysis of the CrowdStrike log identified Ridley accessing a file named “Service report technical notes – ver.3.docx” from a “HarddiskVolume6” contained within a “Nalco Water Files” folder on August 17, 2021 as seen in the screenshot below.

```
</result>
<result offset='1324498'>
  <field k='_time'>
    <value><text>2021-08-17T15:06:52.955+0000</text></value>
  </field>
  <field k='name'>
    <value><text>GenericFileWrittenV13</text></value>
  </field>
  <field k='TargetFileName'>
    <value><text>\Device\HarddiskVolume6\Nalco Water Files\service report notes\~Service report technical notes - ver.3.docx</text></value>
  </field>
</result>
<result offset='1324499'>
```

66. However, forensic analysis of the CrowdStrike log revealed no evidence whatsoever of this “Service report technical notes – ver.3.docx” file being deleted.

67. The Vaughn report makes no reference whatsoever to this file, or any other file being deleted. In my opinion, file deletion of files stored on external USB drives is a significant human activity and further undermines Vaughn’s assertion to the contrary.

68. On page 353 of the Ridley deposition, Ridley claims that the three thumb drives turned over to Tyger Forensics were never connected to any device.

THE WITNESS: As I stated, the three thumb drives, once they were found, were set aside

MR. WALTON: Okay.

THE WITNESS: -- and were not reconnected to any device.

69. As stated above, forensic analysis of the CrowdStrike log identified evidence of Ridley connecting two of the three USB drives to the wiped ChemTreat laptop. The UDisk drive

contained deleted documents containing the Nalco logo and the term “confidential” and the second generic USB drive connected to the wiped ChemTreat laptop contained the file “Ridley Contacts.CSV”; a file which Ridley deleted on February 9, 2022 using a yet undisclosed computer. Therefore, Ridley is indisputably incorrect in stating that two of the three USB drives provided to Tyger Forensics “were not reconnected to any device.”

### **Significant Deficiencies in the James Vaughn Test of CrowdStrike**

70. James Vaughn states on page 53 of his report that he “wanted to validate that a CrowdStrike log created after the reformatting of a laptop is capable of capturing all of the user’s interactions with documents from external devices predating that reformatting.” James Vaughn goes on to conclude that “Based on those validation procedures, I was able to confirm that CrowdStrike logs all interactions a subject laptop has with any documents accessed from an external device, and retains that information even after the subject laptop is reformatted.”

71. However, on page 39 of his report, James Vaughn admits that he limited his “user interactions” to “(1) plugging in an external USB and opening files from that USB using Microsoft Office and PDF applications; (2) plugging in an external USB and opening files from that USB using Windows Explorer; and (3) plugging in an external USB, opening and then saving files from that USB to the test laptop’s hard drive. “

72. James Vaughn never tested printing files stored on external USB devices. Forensic analysis of the CrowdStrike test laptop created by James Vaughn revealed the fact that he never connected a printer to the test laptop. Forensic analysis of the metadata of the test files James Vaughn used in conjunction with the test laptop prove he never printed the test files.

73. Forensic analysis of the test laptop revealed the fact that James Vaughn never tested attaching files to emails and sending the files as email attachments.



74. Forensic analysis of the test laptop revealed the fact that James Vaughn never tested uploading files stored on external USB devices to a cloud storage account.

75. Forensic analysis of the test laptop revealed the fact that James Vaughn never tested copying and pasting content from the test files stored on the USB drive to newly created files on the test laptop.

76. Forensic analysis of the test laptop revealed the fact that James Vaughn never tested deleting files from the USB drive attached to the test laptop as Ridley testified to having performed in his deposition.

77. Forensic analysis of the test laptop revealed the fact that James Vaughn never tested adding multiple files to a ZIP archive file.

78. Ridley's own sworn testimony describes significant file interactions including searching, accessing, segregating and deleting multiple files on multiple different dates. None of these significant file interaction activities testified to by Ridley can be found in the CrowdStrike log. Mr. Vaughn himself does not address in his report these file interactions testified to by Ridley. Vaughn's own "test" process omits testing multiple types of significant file interaction activities such as file deletion Ridley himself testified to having performed.

79. Given the aforementioned omissions from James Vaughn's testing process and Ridley's own sworn testimony, I strenuously disagree with his conclusion that that "CrowdStrike logs all interactions a subject laptop has with any documents accessed from an external device" as clearly he did not test all types of normal file interactions Ridley could have used to access Ecolab information from the external USB devices connected to the wiped ChemTreat laptop, including significant types of file interactions Ridley himself testified to having performed.

80. James Vaughn would have us believe the CrowdStrike tool is a sufficient substitute for forensic analysis of the wiped ChemTreat laptop. It is most certainly not as the CrowdStrike log is an endpoint security malware protection tool, not a data loss prevention tool.

81. Analysis of the CrowdStrike log revealed eight different devices having been connected to the wiped ChemTreat laptop, but James Vaughn's report only references two devices in total.

82. James Vaughn would have us believe that six more devices including the Apple iPad were connected to the wiped ChemTreat laptop, some on multiple different dates, but that no files whatsoever were accessed from those six devices while they were plugged into the wiped laptop because the CrowdStrike tool did not record any related file interactions.

83. However, James Vaughn's test laptop omitted key file interactions such as attaching files stored on an USB drive to an email and sending the email, or deleting files, an interaction which Ridley himself testified to having performed on multiple occasions.

84. Ridley testified that he never owned a personal computer notwithstanding the fact that the UDisk USB drive, which was connected to the wiped ChemTreat laptop on multiple dates, contains Nalco confidential information, and contains evidence that Ridley must have used an undisclosed computer on February 9, 2022 to delete the files contained on the UDisk drive, including a folder named **"Files from Ridley's personal computer."**

85. I have no reasonable explanation why James Vaughn never interviewed Anthony Ridley, nor bothered to analyze the Western Digital drive or any of the other seven devices connected to the wiped ChemTreat laptop, or Ridley's personal Microsoft email account and personal OneDrive contents other than such analysis would have been extremely detrimental to ChemTreat.

### The Western Digital Drive

86. On May 11, 2023, I was provided with a Western Digital My Book 1130, serial number WCAZA5437976, USB serial number 5743415A4135343337393736 with a capacity of 2 terabytes, reported to belong to Anthony Ridley (“WD Drive”) to perform forensic analysis and report on my findings. My forensic analysis results of the WD Drive revealed significant spoliation destruction of the contents of the WD Drive by a person I assume to be Anthony Ridley on February 14, 2022 at 5:08:58 PM CST using an undisclosed computer.

87. Forensic analysis of the CrowdStrike log contains evidence that the WD drive was connected to Ridley’s wiped ChemTreat laptop on nine different days including **July 21, 2021, August 17, 2021, August 18, 2021, August 20, 2021, August 21, 2021, August 22, 2021, December 12, 2021, January 28, 2022 and January 30, 2022** as seen in the screenshots below taken directly from the CrowdStrike log.

### **WD Drive Connected to the Wiped ChemTreat Laptop on July 21, 2021**

```
</result>
<result offset='1444793'>
  <field k='_time'>
    <value><text>2021-07-21T20:54:08.154+0000</text></value>
  </field>
  <field k='name'>
    <value><text>DcUsbDeviceConnectedV2</text></value>
  </field>
  <field k='DeviceManufacturer'>
    <value><text>Western Digital</text></value>
  </field>
  <field k='DeviceProduct'>
    <value><text>My Book 1130</text></value>
  </field>
  <field k='DeviceSerialNumber'>
    <value><text>5743415A4135343337393736</text></value>
  </field>
</result>
```

### **WD Drive Connected to the Wiped ChemTreat Laptop on August 17, 2021**

```
</result>
<result offset='1329405'>
  <field k='_time'>
    <value><text>2021-08-17T12:12:52.730+0000</text></value>
  </field>
  <field k='name'>
    <value><text>DcUsbDeviceConnectedV2</text></value>
  </field>
  <field k='DeviceManufacturer'>
    <value><text>Western Digital</text></value>
  </field>
  <field k='DeviceProduct'>
    <value><text>My Book 1130</text></value>
  </field>
  <field k='DeviceSerialNumber'>
    <value><text>5743415A4135343337393736</text></value>
  </field>
</result>
```

**WD Drive Connected to the Wiped ChemTreat Laptop on August 17, 2021 and August 18,**

**2021**

```
</result>
<result offset='1328544'>
  <field k='_time'>
    <value><text>2021-08-17T12:16:54.170+0000</text></value>
  </field>
  <field k='name'>
    <value><text>DcUsbDeviceConnectedV2</text></value>
  </field>
  <field k='DeviceManufacturer'>
    <value><text>Western Digital</text></value>
  </field>
  <field k='DeviceProduct'>
    <value><text>My Book 1130</text></value>
  </field>
  <field k='DeviceSerialNumber'>
    <value><text>5743415A4135343337393736</text></value>
  </field>
</result>

</result>
<result offset='1324088'>
  <field k='_time'>
    <value><text>2021-08-18T09:05:51.738+0000</text></value>
  </field>
  <field k='name'>
    <value><text>DcUsbDeviceDisconnectedV2</text></value>
  </field>
  <field k='DeviceManufacturer'>
    <value><text>Western Digital</text></value>
  </field>
  <field k='DeviceProduct'>
    <value><text>My Book 1130</text></value>
  </field>
  <field k='DeviceSerialNumber'>
    <value><text>5743415A4135343337393736</text></value>
  </field>
</result>
```

**WD Drive Connected to the Wiped ChemTreat Laptop on August 20, 2021 through August 22, 2021**

```
</result>
<result offset='1316156'>
  <field k='_time'>
    <value><text>2021-08-20T00:12:42.701+0000</text></value>
  </field>
  <field k='name'>
    <value><text>DcUsbDeviceConnectedV2</text></value>
  </field>
  <field k='DeviceManufacturer'>
    <value><text>Western Digital</text></value>
  </field>
  <field k='DeviceProduct'>
    <value><text>My Book 1130</text></value>
  </field>
  <field k='DeviceSerialNumber'>
    <value><text>5743415A4135343337393736</text></value>
  </field>
</result>

</result>
<result offset='1314647'>
  <field k='_time'>
    <value><text>2021-08-22T19:15:10.932+0000</text></value>
  </field>
  <field k='name'>
    <value><text>DcUsbDeviceDisconnectedV2</text></value>
  </field>
  <field k='DeviceManufacturer'>
    <value><text>Western Digital</text></value>
  </field>
  <field k='DeviceProduct'>
    <value><text>My Book 1130</text></value>
  </field>
  <field k='DeviceSerialNumber'>
    <value><text>5743415A4135343337393736</text></value>
  </field>
</result>
```



**WD Drive Connected to the Wiped ChemTreat Laptop on December 12, 2021**

```
</result>
<result offset='540466'>
  <field k='_time'>
    <value><text>2021-12-12T21:20:08.269+0000</text></value>
  </field>
  <field k='name'>
    <value><text>DcUsbDeviceConnectedV2</text></value>
  </field>
  <field k='DeviceManufacturer'>
    <value><text>Western Digital</text></value>
  </field>
  <field k='DeviceProduct'>
    <value><text>My Book 1130</text></value>
  </field>
  <field k='DeviceSerialNumber'>
    <value><text>5743415A4135343337393736</text></value>
  </field>
</result>
```

**WD Drive Connected to the Wiped ChemTreat Laptop on January 28, 2022**

```
</result>
<result offset='239988'>
  <field k='_time'>
    <value><text>2022-01-28T07:29:00.267+0000</text></value>
  </field>
  <field k='name'>
    <value><text>DcUsbDeviceConnectedV2</text></value>
  </field>
  <field k='DeviceManufacturer'>
    <value><text>Western Digital</text></value>
  </field>
  <field k='DeviceProduct'>
    <value><text>My Book 1130</text></value>
  </field>
  <field k='DeviceSerialNumber'>
    <value><text>5743415A4135343337393736</text></value>
  </field>
</result>
```

**WD Drive Connected to the Wiped ChemTreat Laptop on January 30, 2022**

```
</result>
<result offset='229026'>
  <field k='_time'>
    <value><text>2022-01-30T20:46:24.974+0000</text></value>
  </field>
  <field k='name'>
    <value><text>DcUsbDeviceConnectedV2</text></value>
  </field>
  <field k='DeviceManufacturer'>
    <value><text>Western Digital</text></value>
  </field>
  <field k='DeviceProduct'>
    <value><text>My Book 1130</text></value>
  </field>
  <field k='DeviceSerialNumber'>
    <value><text>5743415A4135343337393736</text></value>
  </field>
</result>
```

88. As a first step, I used an industry standard forensic imaging tool, a Tableau model TX1, serial number 000ecc5801f066, to generate a write-protected physical bit-for-bit forensic image of the WD Drive. Forensic images of the WD Drive have been provided to ChemTreat's forensic expert James Vaughn and Anthony Ridley's forensic expert Andrew Rapelovich.

89. To enable me to perform forensic analysis of the WD Drive, I used an industry standard forensic tool, Passmark's OSForensics, version 10.0 Build 1012 (64-bit) to generate a forensic database of the contents WD Drive.

90. Forensic analysis revealed that an individual I assume to be Anthony Ridley used a free to use application named CCleaner to wipe the contents of the WD Drive's "master file table" on February 14, 2022 on 5:08:58 PM CST. According to Microsoft, "All information about a file, including its size, time and date stamps, permissions, and data content, is stored either in MFT



entries, or in space outside the MFT that is described by MFT entries<sup>4</sup>,” meaning the master file table contains references to all file names stored on a given hard drive such as the WD Drive. Therefore, CCleaner wiped all master file table references to file names which existed on the WD Drive prior to February 14, 2022 on 5:08:58 PM CST.

91. I have attached an exhibit generated by OSForensics and containing all 131,211 files CCleaner wrote over the WD Drive’s master file table to destroy file names formerly contained within the WD Drive beyond recovery as **Exhibit H**.

92. Forensic analysis of the WD Drive revealed the fact that the majority of the WD Drive has been overwritten with zeroes as seen in the screen shot below taken directly from the OSForensics database of the WD Drive itself. CCleaner is capable of overwriting hard drive contents with zeroes in order to destroy files beyond recovery.

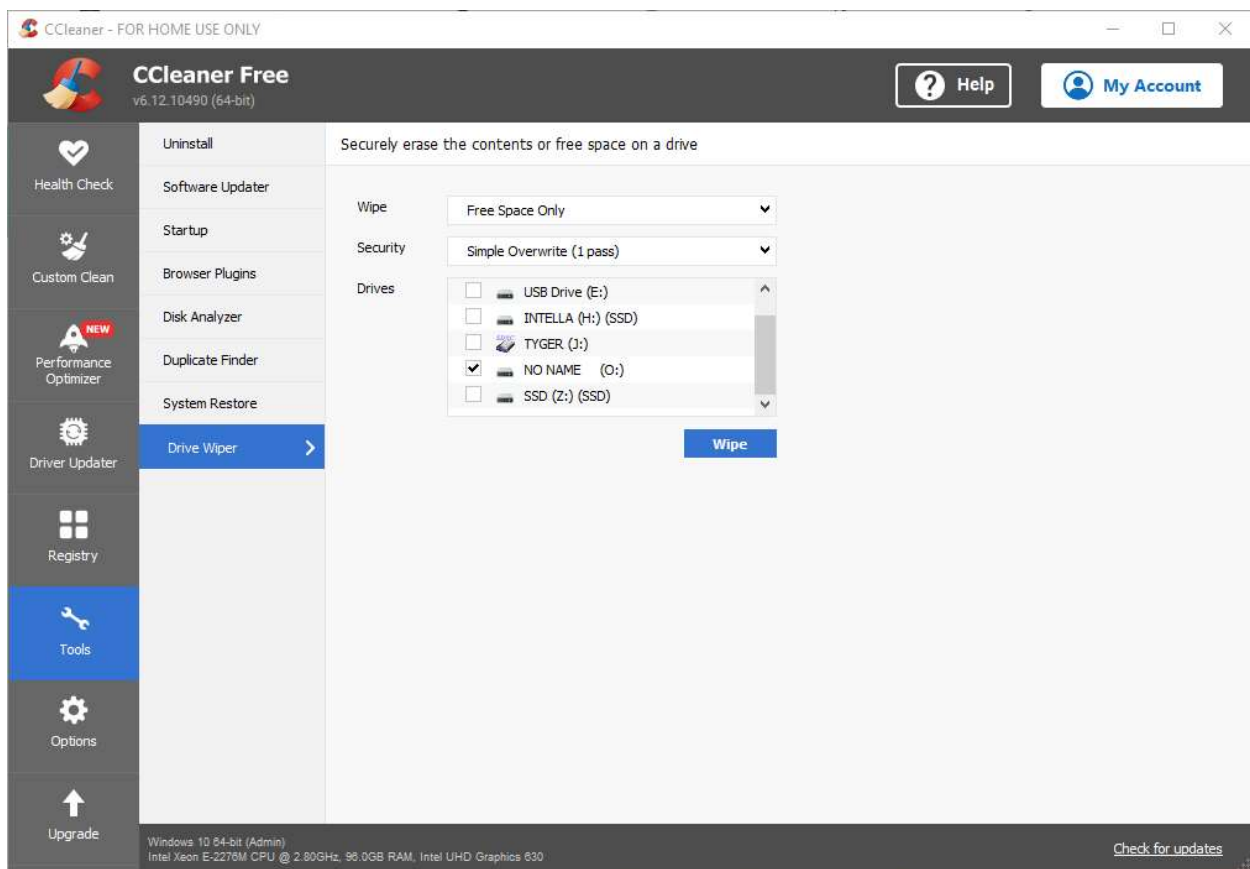
---

<sup>4</sup> <https://learn.microsoft.com/en-us/windows/win32/fileio/master-file-table>

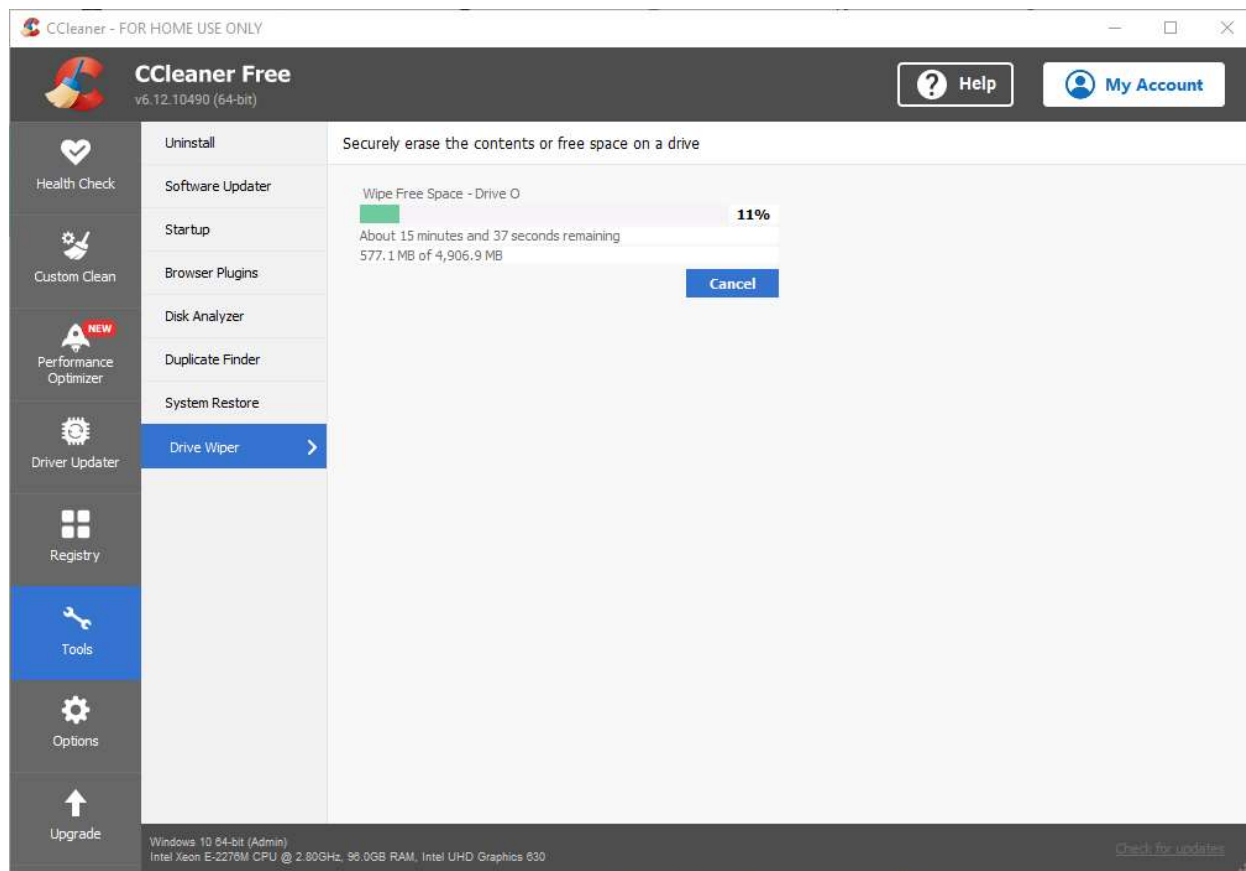


93. I tested CCleaner myself on a USB drive to replicate the results my analysis of the Ridley WD Drive uncovered. CCleaner is a software tool one must take multiple steps to utilize including downloading and installing the software, selecting “Tools” and then “Drive Wiper,” selecting the specific drive one wants to wipe, and then clicking on the “Wipe” button.

94. In the screenshot below, one can see that I have selected my test USB drive named “NO NAME” with the assigned drive letter of “O:”, and the option to wipe “Free Space Only,” using the security setting “Simple Overwrite (1 pass). CCleaner provides the option to wipe the “Entire Drive” but I chose the option to wipe “Free Space Only” which will cause CCleaner to overwrite deleted files and a drive’s master file table, not the entire USB drive contents.



95. After selecting the blue “Wipe” button seen in the screenshot above, CCleaner displayed the below screenshot with the language “Wipe Free Space.” As I describe above, the WD Drive’s master file table “MFT” was wiped using CCleaner.



96. After CCleaner finished wiping my test USB drive, I used OSForensics to carve and recover deleted files from my test USB drive, resulting in the screenshot below, taken directly OSForensics. One can clearly see that CCleaner left the same exact forensic artifacts of multiple files named “Z...ZZZ.ZZZ” in the master file table of my test USB drive one sees in the master file table of the WD Drive displayed in **Exhibit H**. The second screenshot below shows the test USB drive’s deleted contents were overwritten by zeroes, just as one sees in the WD Drive. Therefore, it is beyond dispute, that a person I assume to be Anthony Ridley used the tool CCleaner to wipe beyond recovery Nalco Water files from the WD Drive on February 14, 2022.



36



## Raw Disk Viewer

Device to Scan: Drive-O: [Logical Drive (Forensics Mode) {NTFS}] [Config.](#)

Actions ▼

Type search string or hex value (eg. 0xDEADBEEF) and press Enter to search

	00	08
0x00000000278A94E50	0000000000000000	0000000000000000
0x00000000278A94E60	0000000000000000	0000000000000000
0x00000000278A94E70	0000000000000000	0000000000000000
0x00000000278A94E80	0000000000000000	0000000000000000
0x00000000278A94E90	0000000000000000	0000000000000000
0x00000000278A94EA0	0000000000000000	0000000000000000
0x00000000278A94EB0	0000000000000000	0000000000000000
0x00000000278A94EC0	0000000000000000	0000000000000000
0x00000000278A94ED0	0000000000000000	0000000000000000
0x00000000278A94EE0	0000000000000000	0000000000000000
0x00000000278A94EF0	0000000000000000	0000000000000000
0x00000000278A94F00	0000000000000000	0000000000000000
0x00000000278A94F10	0000000000000000	0000000000000000
0x00000000278A94F20	0000000000000000	0000000000000000
0x00000000278A94F30	0000000000000000	0000000000000000
0x00000000278A94F40	0000000000000000	0000000000000000
0x00000000278A94F50	0000000000000000	0000000000000000
0x00000000278A94F60	0000000000000000	0000000000000000
0x00000000278A94F70	0000000000000000	0000000000000000
0x00000000278A94F80	0000000000000000	0000000000000000
0x00000000278A94F90	0000000000000000	0000000000000000
0x00000000278A94FA0	0000000000000000	0000000000000000
0x00000000278A94FB0	0000000000000000	0000000000000000
0x00000000278A94FC0	0000000000000000	0000000000000000
0x00000000278A94FD0	0000000000000000	0000000000000000
0x00000000278A94FE0	0000000000000000	0000000000000000
0x00000000278A94FF0	0000000000000000	0000000000000000
0x00000000278A95000	0000000000000000	0000000000000000
0x00000000278A95010	0000000000000000	0000000000000000
0x00000000278A95020	0000000000000000	0000000000000000
0x00000000278A95030	0000000000000000	0000000000000000
0x00000000278A95040	0000000000000000	0000000000000000
0x00000000278A95050	0000000000000000	0000000000000000
0x00000000278A95060	0000000000000000	0000000000000000
0x00000000278A95070	0000000000000000	0000000000000000
0x00000000278A95080	0000000000000000	0000000000000000
0x00000000278A95090	0000000000000000	0000000000000000
0x00000000278A950A0	0000000000000000	0000000000000000
0x00000000278A950B0	0000000000000000	0000000000000000
0x00000000278A950C0	0000000000000000	0000000000000000
0x00000000278A950D0	0000000000000000	0000000000000000
0x00000000278A950E0	0000000000000000	0000000000000000
0x00000000278A950F0	0000000000000000	0000000000000000
0x00000000278A95100	0000000000000000	0000000000000000
0x00000000278A95110	0000000000000000	0000000000000000
0x00000000278A95120	0000000000000000	0000000000000000
0x00000000278A95130	0000000000000000	0000000000000000
0x00000000278A95140	0000000000000000	0000000000000000
0x00000000278A95150	0000000000000000	0000000000000000
0x00000000278A95160	0000000000000000	0000000000000000
0x00000000278A95170	0000000000000000	0000000000000000
0x00000000278A95180	0000000000000000	0000000000000000
0x00000000278A95190	0000000000000000	0000000000000000
0x00000000278A951A0	0000000000000000	0000000000000000
0x00000000278A951B0	0000000000000000	0000000000000000
0x00000000278A951C0	0000000000000000	0000000000000000
0x00000000278A951D0	0000000000000000	0000000000000000
0x00000000278A951E0	0000000000000000	0000000000000000
0x00000000278A951F0	0000000000000000	0000000000000000
0x00000000278A95200	0000000000000000	0000000000000000

97. Forensic analysis revealed the fact that six hundred and twenty for files were copied to the WD Drive on February 9, 2022 by a person I assume to be Anthony Ridley using an undisclosed computer. I have included a screenshot taken directly from the OSForensics database of the WD Drive showing the files Ridley copied to a folder named “Lauren's Camera Pictures” on the WD Drive on February 9, 2022.

File System Browser			
File View Tools			
USB004-ANTHONY-RIDLEY-0:\My Pictures\Lauren's Camera Pictures			
	Name	Date created	MFT Modify Date
DANON-04160_A0003-2			
USB004-ANTHONY-RIDLEY-0:			
\$Extend			
\$RECYCLE.BIN			
2009 Ridley Family Picture			
AdaptiveCache			
Anthony & Jamie Engages			
Jeff Boyd Pictures			
Kappa Sigma Information			
My Music			
My Pictures			
804LX8B	DSCF1921.JPG	2/9/2022, 16:15:12.3539474	2/9/2022, 16:15:12.4279478
809JOCQF	DSCF1922.JPG	2/9/2022, 16:15:11.6947465	2/9/2022, 16:15:12.0535471
809OGVQZ	DSCF1921.JPG	2/9/2022, 16:15:11.1175405	2/9/2022, 16:15:11.4762461
818GTFYA	DSCF1920.MOV	2/9/2022, 16:14:57.8887222	2/9/2022, 16:15:08.7931414
821DFGGI	DSCF1919.MOV	2/9/2022, 16:14:52.9747136	2/9/2022, 16:14:56.7655203
823FOLCT	DSCF1918.JPG	2/9/2022, 16:14:52.3039124	2/9/2022, 16:14:52.8187133
8335MFYH	DSCF1917.MOV	2/9/2022, 16:14:39.5098899	2/9/2022, 16:14:49.8075080
834QYQCY	DSCF1916.JPG	2/9/2022, 16:14:38.8390887	2/9/2022, 16:14:39.3382895
8502GQOR	DSCF1915.JPG	2/9/2022, 16:14:38.0746873	2/9/2022, 16:14:38.4667484
853KXKDS	DSCF1914.JPG	2/9/2022, 16:14:37.1542857	2/9/2022, 16:14:37.8406869
854HEBFP	DSCF1913.JPG	2/9/2022, 16:14:36.7798851	2/9/2022, 16:14:37.0498855
858DLRAU	DSCF1912.JPG	2/9/2022, 16:14:36.2182841	2/9/2022, 16:14:36.6394848
869MLXEC	DSCF1911.JPG	2/9/2022, 16:14:35.5943830	2/9/2022, 16:14:36.0466838
87JPGMVM	DSCF1910.JPG	2/9/2022, 16:14:34.9702819	2/9/2022, 16:14:35.4382817
877JGJNU	DSCF1909.JPG	2/9/2022, 16:14:34.2994807	2/9/2022, 16:14:34.7890815
884RY8BK	DSCF1908.JPG	2/9/2022, 16:14:33.6754796	2/9/2022, 16:14:34.0966803
890SODRR	DSCF1907.JPG	2/9/2022, 16:14:33.0398783	2/9/2022, 16:14:33.5038793
898RTWGW	DSCF1906.JPG	2/9/2022, 16:14:32.3806773	2/9/2022, 16:14:32.8642782
900ONROE	DSCF1905.JPG	2/9/2022, 16:14:31.9128765	2/9/2022, 16:14:32.3182772
903FDFID	DSCF1904.JPG	2/9/2022, 16:14:31.5226758	2/9/2022, 16:14:31.8034763
909JHOYA	DSCF1903.JPG	2/9/2022, 16:14:31.2950752	2/9/2022, 16:14:31.4290757
914JLUD	DSCF1902.JPG	2/9/2022, 16:14:30.6802743	2/9/2022, 16:14:31.0546750
924B3KKG	DSCF1901.MOV	2/9/2022, 16:14:18.0286521	2/9/2022, 16:14:28.4962705
929JPUJD	DSCF1900.MOV	2/9/2022, 16:14:05.7826306	2/9/2022, 16:14:15.6574880
938VQGGM	DSCF1899.MOV	2/9/2022, 16:13:57.0466153	2/9/2022, 16:14:04.8136286
949OLYDL	DSCF1898.MOV	2/9/2022, 16:13:45.0179941	2/9/2022, 16:13:55.3930124
954DR1J	DSCF1897.MOV	2/9/2022, 16:13:33.9887747	2/9/2022, 16:13:43.6919918
965FLQHE	DSCF1896.MOV	2/9/2022, 16:13:24.5819582	2/9/2022, 16:13:32.8499717
972CY8KG	DSCF1895.JPG	2/9/2022, 16:13:23.9267570	2/9/2022, 16:13:24.4415579
972JHGMN	DSCF1894.JPG	2/9/2022, 16:13:23.3183560	2/9/2022, 16:13:23.8175968
973MXEPR	DSCF1893.JPG	2/9/2022, 16:13:22.5539546	2/9/2022, 16:13:23.1635857
973PVYFN	DSCF1892.JPG	2/9/2022, 16:13:21.7583532	2/9/2022, 16:13:22.4291544
980M9CTP	DSCF1891.JPG	2/9/2022, 16:13:21.3998526	2/9/2022, 16:13:21.6959531
983KCA3H	DSCF1890.JPG	2/9/2022, 16:13:20.6819513	2/9/2022, 16:13:21.2279523
986JWOWX	DSCF1889.JPG	2/9/2022, 16:13:20.4947510	2/9/2022, 16:13:20.6507513
991XEVVB	DSCF1888.JPG	2/9/2022, 16:13:20.2763506	2/9/2022, 16:13:20.4479509
backup	DSCF1887.JPG	2/9/2022, 16:13:19.8863499	2/9/2022, 16:13:20.1983505
Boyd Pictures	DSCF1886.JPG	2/9/2022, 16:13:19.1375486	2/9/2022, 16:13:19.7615497
Building pictures	DSCF1885.JPG	2/9/2022, 16:13:18.4355474	2/9/2022, 16:13:18.9971484
Family Pictures	DSCF1884.JPG	2/9/2022, 16:13:17.7169461	2/9/2022, 16:13:18.3263472
gun and serial number	DSCF1883.JPG	2/9/2022, 16:13:16.9359447	2/9/2022, 16:13:17.5609458
Harley and Bike Week	DSCF1882.JPG	2/9/2022, 16:13:16.4523438	2/9/2022, 16:13:16.8111444
Harrison's 40th Birthday	DSCF1881.JPG	2/9/2022, 16:13:16.0155430	2/9/2022, 16:13:16.3899437
www.antonio.com	DSCF1880.JPG	2/9/2022, 16:13:15.4061419	2/9/2022, 16:13:15.8897428
	DSCF1879.JPG	2/9/2022, 16:13:14.8279408	2/9/2022, 16:13:15.2969417
	DSCF1878.JPG	2/9/2022, 16:13:14.2195398	2/9/2022, 16:13:14.7187406
	DSCF1877.JPG	2/9/2022, 16:13:13.6111387	2/9/2022, 16:13:14.0947395
	DSCF1876.JPG	2/9/2022, 16:13:13.0339377	2/9/2022, 16:13:13.5019385
	DSCF1875.JPG	2/9/2022, 16:13:12.4603362	2/9/2022, 16:13:12.8779374
	DSCF1874.JPG	2/9/2022, 16:13:11.5207350	2/9/2022, 16:13:12.0355359
	DSCF1873.JPG	2/9/2022, 16:13:10.9903341	2/9/2022, 16:13:11.4115348

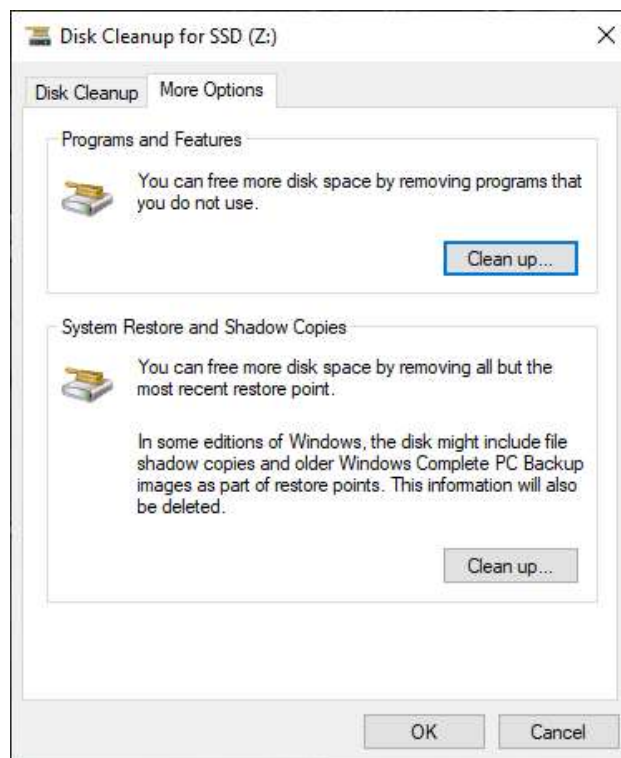
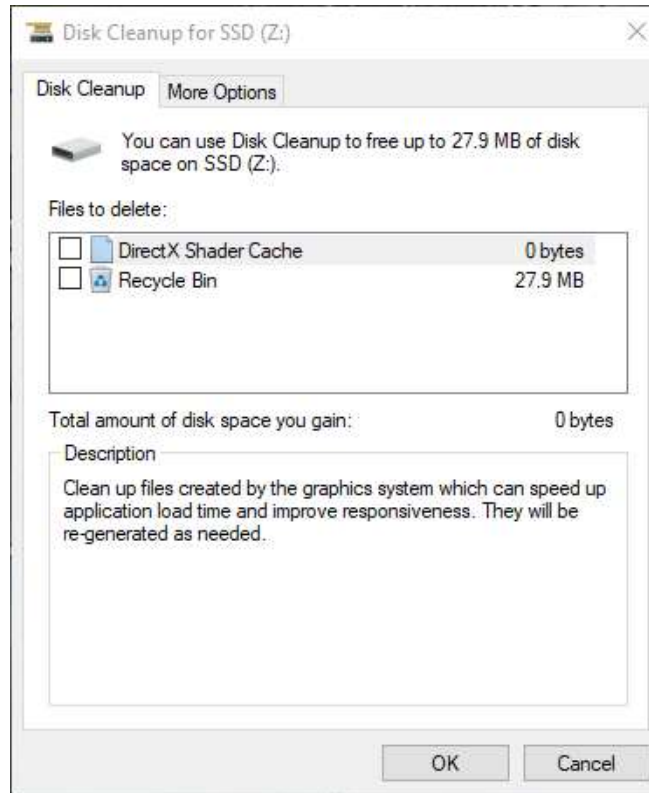


98. Forensic analysis of Ridley's second ChemTreat laptop, a Dell Latitude 5320, serial number HC28DL3 ("Second ChemTreat Laptop"), revealed the fact that the WD Drive was never connected to this Second ChemTreat Laptop.

99. Forensic analysis of the CrowdStrike log revealed the fact that the WD Drive was last connected to the wiped First ChemTreat Laptop on January 30, 2022.

100. Therefore, Ridley must have used an undisclosed computer on February 14, 2022 to run the program CCleaner and delete and wipe beyond recovery all Nalco Water files and all references to the names of the deleted Nalco Water files formerly residing on the WD Drive.

101. On page 101 of Ridley's deposition, Ridley testified that he used Microsoft's Disk Cleanup Utility to overwrite deleted files on the WD Drive. However, I tested Microsoft's Disk Cleanup Utility myself and determined that Microsoft's Disk Cleanup Utility does not result in the forensic artifacts one sees on WD Drive. As seen in the screenshots below of Microsoft's Disk Cleanup utility, there is no option to wipe a drive, only empty the Recycle Bin and delete "Direct X Shader Cache." For my test, I selected the option to empty the Recycle Bin.




102. I used OSForensics to analyze my test drive, “SSD (Z:)” and determined that Microsoft’s Disk Cleanup Utility does not overwrite master file table entries and in fact does not overwrite the contents of a drive with zeroes. Therefore, there is no evidence that Ridley used Microsoft’s Disk Cleanup Utility on the WD Drive.

### **Conclusion**

103. A person I assume to be Anthony Ridley used a yet undisclosed computer to run the wiping tool CCleaner against the WD Drive on February 14, 2022 to destroy beyond recovery deleted files and all references to the names of deleted Nalco Water files which once existed on the WD Drive.

Dated: June 14, 2022

Respectfully submitted,

A handwritten signature in black ink that reads "Laurence D. Lieb". The signature is written in a cursive style with a horizontal line underneath it.

Laurence D. Lieb